Internet content regulation

d'Udekem-Gevers, Marie; Poullet, Yves

Published in:
The Computer Law and Security Report

Publication date:
2002

Document Version
Publisher's PDF, also known as Version of record

INTERNET CONTENT REGULATION

CONCERNS FROM A EUROPEAN USER EMPOWERMENT PERSPECTIVE ABOUT INTERNET CONTENT REGULATION: AN ANALYSIS OF SOME RECENT STATEMENTS — PART II

Marie d'Udekem-Gevers and Yves Poullet, University of Namur, Belgium

This article, published in two parts, explores the debate between the Bertelsmann Foundation and the Centre for Democracy and Technology about regulation of illegal and harmful content on the Internet. The authors analyse the method, interests and limits of the self-regulatory model proposed by the European Institutions, bearing in mind the perspective of user empowerment. Part II considers the possibilities for a global rating system for content and the prospects of ISPs jointly subscribing to controls over legal content.

7. "PROMOTING A SINGLE, COMPREHENSIVE, GLOBAL RATING SYSTEM"

To prepare the analysis of the Center for Democracy and Technology (CDT) text, let us begin by sketching the technical framework of the filtering services and noting the results of a survey we have carried out on Internet filtering criteria.

7.1. Technical framework

The filtering techniques are:"a means of empowering users by allowing their children to have access to a broad range of content on the Internet while avoiding contact with material that the parent would consider *harmful*".[56] They are varied and complex. Moreover, the filtering services currently available on the market are numerous (more than 100)[57] and comparisons are difficult[58]: each service has its own characteristics. One issue is vagueness: on the one hand, the vocabulary is not universally accepted and frequently not (well) defined and, on the other hand, the technical framework is often not precise.

We will now outline here a general framework.[59] The 'filtering services' are considered *sensu lato* : they include any technical tool available for the end user which is involved in the process of Internet filtering, wherever it is located (PC filtering software packages, server based solutions,) and whatever it performs (providing only a rating criteria definition, providing a rating criteria definition and a rating, both classifying and filtering, filtering on the basis of ratings, etc.)

The scope of Internet control (*see table 2*) can include topics or time. From a technical point of view, the topic control (or 'filtering') can be maintained either at the entry point level or at the content level itself.

At the entry point level, filtering of URLs [Uniform Resource Locator] can be based either on ratings (i.e. labelling) only or on classifications into URL lists (generally 'black' lists [i.e. 'not for kids' lists/'NOT' Lists] or, sometimes, lists of suggested sites) or on both ratings and URL lists. One should note that rating and classifying are conceptually equivalent. Both imply that criteria (for classifying/rating) (for ex. word lists) have been defined beforehand. Both (*see table 3*) can be carried out:

- Either by human reviewers;
- Or by software;
- Or by human reviewers with the help of software.

PICS ratings are the most common. PICS stands for 'Platform for Internet Content Selection'. It is a set of technical standards developed since summer 1995 by the World Wide Web Consortium (W3C).[60]

It should be stated that PICS allows the users to choose their label sources independently of their filtering software. The labelling of a site can be done by third parties (third party rating)[61] or by the content provider him/herself ('self rating').[62] Currently only web sites have received PICS labels. But: "PICS labels *can* describe anything that can be named with a URL.That includes FTP and Gopher. email messages do not normally have URLs, but messages from discussion lists that are archived on the Web do have URLs and can thus be labelled...Usenet newsgroups,[63] and even individual messages, have URLs, and hence can be labelled.There is not yet an official URL scheme for IRC, but the PICS specifications defined a preliminary scheme, and a more robust URL scheme for IRC is being worked on."[64]

Filtering at the content level implies that both rating/classifying and filtering are managed in real time by software. It can be based on lists of words (i.e. in fact on criteria themselves). Currently image recognition by software is only beginning (cf. for example, Image Filter[65] by the firm entitled LookThatUp).The choice of a specific technique has practical results for the final user.

ISSN 0267 3649/02/$20.00

Table 2. Control scopes and corresponding possible technical solutions.

CONTROL GENERAL SCOPES	CONTROL SPECIFIC SCOPES	POSSIBLE CURRENT TECHNIQUE, SOLUTIONS
1.Topic control at the **entry point** (to an address or a file) level (**2 steps**)	1.1 Anything with a URL i.e • **WWW** (HTML Protocol) • FTP (File transfer Protocol) • GOPHER (for information research • Usenet **Newsgroups** and Individual messages (NNTP Protocol) • TELNET (for terminal access) • [IRC Internet Relay Chat] (N.B. email messages do not have URLs)	PICS labelling (self-rating or third party rating) and *filtering*
		Filtering on the basis of black/white **lists of** • **URLs** or • Names of newsgroups, chat etc.
	1.2 Local or online applications e.g. games, personal financial managers etc.	Filtering on the basis of lists of application names/ addresses
2.Topic C Control at the **content** level itself (**1 step in real time**)	2.1 Incoming information 2.1.1 Anything with a URL 2.1.2 (Without a URL) N.B. for example, via email (including their attachments)	**Lists of words (=criteria)** + • Key word/string filter (or word-matching)/ • Artificial intelligence based software
	2.2 (Outgoing information (for ex.-personal information via IRC, Website questionnaire, email etc. or *offensive* words in search of sexually explicit sites or conversations))	
3. **Time** Control	3.1 Hours/day 3.2 Days/week 3.3 Total by week	

Three main qualities of the filtering techniques have to be considered (*see table 3*):

- 'Reliability', defined as the capacity to take into account the context of a given content;
- 'Scalability', i.e. the capacity to manage the increasing number of web sites; and
- 'Adaptability' which is considered in this paper as the capacity to cope with the evolution and the possible changes of a given web site.

Control at the entry point level with rating/classification by human reviewers is the most reliable but the less scalable and adaptable. Fully automatic control in real time has the lowest reliability and the highest scalability and adaptability. At present, it is unclear which system will be preferred. As pointed out by the Commission on Child Online Protection, (2000, p. 42-43), "No particular technology or method provides a perfect solution, but when used in conjunction with education, acceptable use policies and adult supervision, many technologies can provide improved safety from inadvertent access from harmful to minors materials."

Some filtering services are dedicated to a specific control (for example, time control or E-mail filtering). But frequently,

Table 3. Technical solutions and their consequences.

CONTROL SCOPES	TECHNICAL SOLUTIONS		CONSEQUENCES
Topic control	Control at the entry point level → 2 steps Rating/classifying	• By human reviewers	***Highest 'reliability'*** Low 'scalability' Low 'adaptability'
		• By human reviewers with the help of software	
		• By software only (web crawler)	
	Control at the level of the content itself → 1 step	Fully automatic in real time	Low 'reliability' ***Highest 'scalability'*** ***Highest 'adaptability'***

Table 4. Summary of those who defined the filtering criteria (in 22 filtering services with a list to block access (not linked to PICS)).

IDENTIFICATION OF THE PEOPLE/BODY RESPONSIBLE FOR DEFINITIONS	NUMBER	LOCATION
Commercial firm	20 (but 2 with social concerns)	• 28 USA (5: California) • 2: Canada
Non-profit organization	1	USA
Private individual	1	

an off-the-shelf filtering service provides several technical solutions for example, time control and topic control; control of topic at the entry point level and also at the content level; etc. Moreover, some services also include the control of outgoing information or of on-line applications (*see table 2*).The current market offer is very diverse.

7.2. Summary of our survey on Internet filtering criteria

In this section we will look at the results of a survey[66] carried out by one of the authors of this paper in 1998 and the beginning of 1999.

7.2.1. Introduction

This survey analyzes a large sample of current off-the-shelf filtering services to be used in the home or in the school or even now in companies. It focuses mainly on 'topic' filtering services (*see table 2*) and, particularly, on the access control to Internet sites[67] (i.e. anything with a URL [Uniform Resource Locator]).As a rule, the providers of the filtering services base it on the documentation (sometimes including a 'demo' put on the WWW). Occasionally, this documentation has been completed by analysing the downloaded filtering software itself or by email correspondence with the provider. Filtering services totally devoted to firms or with insufficient documentation are not considered.

The survey concerns a sample of 44 filtering services. Among them, 9 are PICS rating services.Among the 35 other services, 31 are partially or totally based on URL/word/(other) YES/NOT lists and, among these 31, 22 are partially or totally based on NOT lists.Among the roles implicated by any Internet (URLs) filtering process as defined by Resnick (1998) (see § 4.1), three are linked to filtering criteria: to define the criteria,[68] to use them to rate/classify and to customize (or select) them.

7.2.2. Filtering services with a list to block

In the studied sample of 22 filtering services with a list to block access to Web sites, classification criteria (*see table 4*) were mostly (20/22) *fixed* by the commercial firm which provides the filtering service. With the exception of two Canadian corporations, all these firms (i.e. 18) are located in US, frequently in California (5/20). Languages other than English were rare. On the other hand, 16 of the 17 filtering services mainly based on URL NOT Lists are themselves (either directly via the staff or indirectly via a software) responsible for classification of the web sites, on the basis of the defined criteria. In the sample of three filtering services working in real-time with artificial intelligence, the classification/rating is, by definition fully automatic, i.e. performed by a software written by the firm.

At this stage, customization here can occur at two levels: classification criteria definition or URL. In the sample of 17 filtering services mainly based on URL NOT Lists:

- One gives full control to the final user without any predefinition;
- One provides the possibility of both adding to [or deleting] predefined criteria and of adding [or deleting] a URL (very high level of customization);
- Six provide a choice of predefined criteria plus the possibility to add [or delete] an URL (high level of customization);
- Six provide a choice of predefined criteria (only);
- Two only provide fully customizable and visible NOT lists
- One provides only the possibility of adding/deleting a URL to/from the NOT lists;
- One does not provide any possibility of customization.

In the sample of three filtering services working in real-time with artificial intelligence:

- Three allow the list of words to be modified;
- One provides the possibility of adding an URL to a NOT List.

We can conclude that the analysed filtering services based on NOT lists provide the possibility of customization (and sometimes of extensive customization) but this customization

Table 5. Summary of those who defined the filtering criteria (in the sample of 9 PICS rating services).

IDENTIFICATION OF THE PEOPLE/BODY RESPONSIBLE FOR DEFINITION	NUMBER	LOCATION
Commercial firm	4	• 2 USA • 2 Canada
Non-profit organization	4	• 3 USA • 1 Italy
Private individual	1	• UK

Table 6. Synthesis of those who classify (in the sample of 9 PICS rating services).

IDENTIFICATION OF THE PEOPLE/BODY RESPONSIBLE FOR CLASSIFICATION	NUMBER	METHOD
Self Rating	6	N/A
Third party PICS rating services	3	• 1 (Currently non-profit): mainly artificial intelligence • 2 Do not carry out the labelling themselves but employ people to do it.

can only be brought into play in categories predefined by the firm and in lists made by the firm. Let us add that the URL lists are, for the most part, undisclosed.

7.2.3. PICS ratings

As shown in *table 5,* those who set the criteria definition in the sample of PICS rating services analysed in 1998—99 were nearly all located in North America. All but one set of criteria was defined in English.

On the other hand, among the three third party ratings, one rates via artificial intelligence and the other two do not carry out the labelling themselves but employ people to do so (*see table 6*).

With PICS, the customization/definition of filtering criteria can currently occur at 3 levels:

- Choice of the rating source(s) (one or several);
- Choice of the criteria available in the rating source(s);
- Choice of the criteria levels (if any).

In future, it could be possible to use *profiles* (i.e. predefined filtering customizations)

7.2.4. Ethical viewpoint

To 'fix criteria for rating/classifying' is not value-neutral and to 'rate/classify' can imply moral judgements. From an ethical point of view, it is thus very important that the final user (parent, teacher,) can currently either do it him/herself (but this could be a very big undertaking) or find both criteria and a rating/classification in accordance with his /her own value judgements.[69] This last choice should be easier with PICS since this standard allows the users to select their filtering software and their label sources independently.

In the sample we have analysed, *the observations made are ethically worrying*. First, outside PICS, moral issues are obvious: the user is linked to the value judgements of the firm providing the filtering service (including the classification criteria and the classification itself into usually hidden lists). Firms claim they give control to the parents (or teachers). In fact, the firms themselves have the control. Moreover, the available categories for filtering reflect mainly US values. Obviously, European users will not find that they suit their own cultural diversity. As to customization, it could require time and some expertize.

In PICS ratings, the situation is a little less negative than in other filtering services of the sample. The majority of criteria definitions are set outside the framework of firms and nearly half of them, outside US However, all but one is in English! Moreover, these PICS services are still rare. And few filtering software applications can use them. The possibility, offered by PICS, of providing cultural diversity and independence from firms from the value judgement viewpoint, has not (yet?)[70] been fully exploited. On the other hand, with PICS, the customization ('profiling')[71] could be carried out, in the future, by a third party chosen by the parents, and these would then only have to select the required age according to each of their children.

7.3. CDT text analysis

One of the two threats to free speech by the Bertelsmann Memorandum is condemned by CDT as follows: "The Memorandum recommends the widespread adoption of a single uniform rating system to be used by content creators to enable 'better' filtering. We disagree with several assumptions underlying this recommendation and believe that its adoption would likely result in several undesired outcomes, most notably the drive toward a single *mandatory*[72] labelling system. We urge that this recommendation be revisited." We will now analyse, step by step, the arguments developed by CDT. This argument is divided into two parts:

- "The relationship among rating, labelling and filtering";
- "A market failure or a growing, but not yet perfect, market response?"

7.3.1. "The relationship among rating, labelling and filtering"

In the first paragraph, CDT is perfectly right when it declares: "while some filters use self-rating [...] others are not dependent upon the existence of labels or ratings (either self or third-party). Filters make decisions about content based on many different kinds of attributes [...] Frequently several of these methods are combined in a filtering tool. This variety and polymorphism characterize the current state of the off-the-shelf filtering services (see § 7.1). And this text is justified when pointing out that the Memorandum fails to include current diversity and focuses only on the rating solution. Moreover the Memorandum does not make clear that this solution does not cope with data without URLs (such as E-mail etc.). That is another problem insofar as the Memorandum has focused its attention only on web sites control.

CDT is obviously right again when claiming, in the second paragraph: "Much of the content that filters are designed to exclude from view is created by individuals who are not interested in having their message screened from view." The issue of the unlabelled sites is indeed a major one in the Memorandum solution. If the filtering service does not block unrated sites, then the global control will not be efficient but if it does, then

Table 7. Filtering and rating techniques: different concerns and conflicting interests.

USER (=*PARENT*) EMPOWERMENT TO CONTROL CONTENT		*CONTENT PROVIDER* FREE SPEECH
1. *Respect for personal and cultural values* → Rating/filtering vocabulary(/ies) defined by independent non-profit organization(s) (as suggested by the Bertelsmann Foundation) → Rating by various independent non-profit organizations (↔ self rating as suggested by the Bertelsmann Foundation) → Possibility of customization by various independent non-profit organizations (cf. for example 'templates' as suggested by the Bertelsmann Foundation.) → Choice for the user of filtering or not filtering Internet content.		
2.*Technical diversity* (as advocated by CDT)		
3. *Efficiency* of the various filtering techniques: (notably) maximization of the number of labelled sites → Creation (by governments[74]) of incentives for rating (as suggested by the Bertelsmann Foundation) or even *compulsory labelling*. → A single rating vocabulary (?) (as suggested by the Bertelsmann Foundation.)	↔	*No compulsory labelling* (as advocated by CDT)

innocuous and very interesting sites will be not accessible.[73] And thus in this case, as noted by Weinberg (1997), blocking software could end up blocking access to a significant amount of the individual, idiosyncratic speech that makes the Internet a unique medium of mass communication. Filtering software, touted as a speech-protective technology, may instead contribute to the flattening of speech on the Internet. The Memorandum proposal envisages to providing the possibility of downloading white lists of sites which will be treated as acceptable, irrespective of rating.This is an interesting solution, but only a partial one.

But the technical explanations given by CDT on "filters … that do not require the cooperation of content providers" in its third paragraph are unclear. In fact, with self rating, any filtering service — i.e.: PICS labelling by a third party (solution not mentioned in CDT's paper), filtering on the basis of lists of URLs or names and filtering real time — implies to non-involvement of content providers. On the other hand, the only solution to cope efficiently with the increase in the number of web sites is control in real time at the content level (see § 7.1). And with the Internet's current exploding evolution, this 'scalability' can be considered by some people as paramount.

The next paragraph is of paramount importance for the argument of CDT and for our discussion. On the one hand, it explains the main concern of this organization: "This [global cooperative filtering system suggested by the Bertelsmann Memorandum] raises the spectre of mandatory labelling, for without mandatory labelling, a substantial portion of the content will likely remain unlabelled. But mandatory labelling is a form of forced speech, and therefore an infringement on the freedom of expression." One should note that, contrary to the concern put forward in its paper title, CDT defends *content providers'* free speech but *not parents*' empowerment (*see table 7*).The Interests of parents and of the media (or content providers) are in conflict. From a final user empowerment perspective, creation by governments of incentives for rating or even mandatory labelling could be considered as a good initiative! The more sites labelled with a standard, the more efficient any filtering services based on this standard.

On the other hand, in the fourth paragraph CDT cites an advantage but presents it as negligible and unimportant: "cooperative filtering could possibly enable individuals to more carefully tailor filters to reflect their values…" In the CDT text, this advantage is presented in a few words, and is not explained. But this could be considered as basic and fundamental to the empowerment of parents (*see table 7*). Indeed, *respect for personal values and for cultural diversity should not be neglected on the pretext of free speech, particularly in European countries.*[75] European Union authorities indeed are very sensitive to the cultural differences between their members (see § 6.1). And from a final user point of view, respect for values is probably more important than technical diversity provided by the market.

We will now examine in further detail this advantage which is somewhat neglected by CDT. First, one should note that this possibility is offered not only by the so-called 'cooperative filtering' (i.e. mainly based on PICS self-ratings) but also by third party PICS ratings: from the point of view of respect of values, the PICS contribution is fundamental. Indeed, this standard allows the users to choose their label sources independently of their filtering software. (See § 7.1.). It is worth noting here one of the conclusions[76] of the US Commission on Child Online Protection (2000 p.42): "rating and labelling may have positive synergistic effects on other technologies, such as filtering. The use of such systems could have significant impacts on consumer empowerment."

We do not completely agree with CDT when it claims in the fifth paragraph: "a diverse environment of user empowerment tools including filters, some of which use rating and labelling systems, is more likely to provide parents with effective control over content considered potentially inappropriate for some children […]." We admit that the technical diversity

provided by the current market could help parent empowerment as far as it does not result in parents' confusion. But we think that an effective control over URL sites content implies first and foremost for the parents that the three roles (see 7.2.1 and *table 7*) linked to filtering criteria (to define the criteria, to use them to rate/classify and to customize (or select) them) are fulfilled in accordance with their own values. We think also that the filtration criteria must be defined outside industry and by independent third parties. The shelf filtering services do not cope currently with these requirements.

To sum up, it must be pointed out that, from the point of view of an effective control by parents, the solution suggested by the Memorandum has several advantages (*see table 7*).

- First, it plans to entrust the responsibility for defining the selection criteria (i.e. "the initial basic vocabulary", according to the terms of the Memorandum) to a non-profit and independent organization: "not under the auspices or control of any particular business organization."(See The Memorandum p.35). This point is worth underlining. Indeed defining the criteria is a crucial role. First, it automatically influences subsequent steps of the filtering process (assigning labels and selecting filtering criteria). But, as pointed out by CPSR (1998),[77] "in general, the use of a filtering product involves an implicit acceptance of the criteria used to generate the ratings involved [...] Parents should take care to insure that the values behind the ratings are compatible with their beliefs." But will it be possible to collect enough criteria and to specify them with sufficient nuances to reflect all the different European cultures?
- Secondly, the Memorandum solution entrusts to third parties to selection of criteria (i.e. "the production of templates", according to the vocabulary of Bertelsmann) "that match their particular set of values and beliefs". Thus it aids parents in this task: they will have only to choose a relevant template.[78]
- Thirdly, the solution of "a single comprehensive rating system" is conceptually of interest: the more extended a standard is, the more useful it is for the users. A frequently used vocabulary standard should provide benefits both at the level of rating and the level of criteria selection. The challenge with this solution will be to define a vocabulary with enough nuances to allow reflection of all the different cultures.

But the solution also has several drawbacks. As pointed out by CDT, the issue of the unlabelled sites[79] remains unsolved. Moreover, it is not a fully satisfactory solution (it has to be completed, if the parents wish, by other tools for example to control ingoing email or outgoing information or to set time limits on children's access).

Another drawback, not criticised by CDT, lies in self-rating: this solution,[80]provides a higher risk of subjective labelling (or even of mislabelling).[81] Nevertheless, a system of liability in case of false or deceptive statements[82] is still possible whenever self-rating is incorrect. In any case, for more objective judgements, third party rating is a better (but sometimes more expansive) solution. Nevertheless the third-party rating solution is not a panacea: it could require additional protection for their users: so, it would be adequate to ensure, through appropriate information on their web sites, a transparency on the persons or associations which are behind the work done and to enforce a system of liability in case of negligent behaviour in the rating of the web sites. Such individuals are still rare (*see table 6*) but, in the future, it seems that they would often be non-profit organizations and would consider this last requirement as impracticable. Third party rating should take place in combination with self-rating.[83] Finally, the proliferation of rating systems could create confusion for the Internet users.

7.3.2. "A market failure or a growing, but not yet perfect, market response?"

The market failure is quite obvious when we look at the recent declaration made by the European Director of ICRA, Ola-Kristan Hoff (2000), which drew attention to the fact that, of the estimated total of about two billion web sites, only 150 000 web sites have been currently rated with RSACi labels. It is clear that the quality and success of the filter depend on the number of classified sites and the correctness of the classification. According to this statement, the Bertelsmann Foundation encourages the adoption of a mandatory filtering system.

CDT analyses the Bertelsmann assertion as follows: "The Memorandum's recommendations for a rating and filtering system are premised on the perception that the market has failed to respond to the user demand for tools to control unwanted content. According to the Memorandum, the central problem appears to be that content providers have failed to rate. The Memorandum [...] proposes the adoption of a single, comprehensive, value-neutral (or objective/descriptive) rating vocabulary, which, it is assumed, will encourage rating and overcome the market's failure." We agree, with the Bertelsmann Foundation, that a single vocabulary would encourage rating but we are not convinced that it will be enough to overcome the market issues.

The CDT claims that: "In the US, the premise to this line of reasoning is incorrect: the market has not failed." It is true that the market provides a technical diversity. But from the point of view of respect for cultural and personal values, our survey (see § 7.2) has shown the market's failure. What is currently offered on the market is not a panacea. One solution to overcome several drawbacks of the market should be to develop filtering based on rating. The solution suggested by the Memorandum and criticised by CDT is good for every data with an URL. And the relative volume of such data on the Internet is very important.

We do agree with this CDT 's claim (paragraph 3) that: "The market response should be judged a success based on the ability of parents to avail themselves of tools *that reflect a diversity of views* regarding what is and is not appropriate for a child of a given age." We disagree entirely with the conclusion following the previous claim: "The industry is moving to address this need — in a decentralized, market-driven manner". Our survey (see § 7.2) has shown that an attitude of "laissez-faire" towards the market seems not to be the best solution.

In agreement with Grainger, the representative of the Australian Broadcasting authority (ABA) (1999 p.53—54), we believe that: "It is essential for policy makers and legislators, as they [...] prepare new rules for [...] the Internet, to revisit and restate the public interest objectives they believe should apply to those industries and their governance.

Sweeping references to the 'public interest' may be less effective than a clear articulation of the process concerns that legislators are seeking to advance [...]"[84]

With regards to the Internet, free speech (as so frequently underlined in US), the protection of minors, respect for personal values and respect for cultural diversity are among the public interest objects to be achieved.

8. "ENCOURAGING ISPs TO JOINTLY SUBSCRIBE TO CONTROLS OVER LEGAL CONTENT"

8.1. CDT text and Bertelsmann Foundation Memorandum analysis

The CDT analysis of the Bertelsmann Foundation Memorandum concludes that this report might be considered as a way of "encouraging ISPs to jointly subscribe to controls over legal content." One should note that the Bertelsmann Foundation text itself does not use the word 'co-regulation'. But the CDT makes it clear that, according to the Bertelsmann Foundation Memorandum, this control will be exercised in association with public authorities: "Rather than being truly 'self-regulatory', the codes of conduct envisioned in the Memorandum more closely resemble calls for 'joint regulation'…" This coalition between private and public regulators is considered by CDT as a great danger for citizens' fundamental liberties such as the freedom of expression and the privacy.

This interpretation of the Bertelsmann Foundation text is not fully accurate. Considering the role of the codes of conduct to be created by the Internet Industry, the Bertelsmann Foundation Memorandum asserts (p.24) that these codes: "should be endorsed as a front-line mechanism to addressing content issues […] They should distinguish between illegal content and the protection of minors from potentially harmful content." The Memorandum adds (p.22):"Self-regulation cannot function without the support of public authorities, be it that they simply do not interfere with the self-regulatory process, be it that they endorse or ratify self-regulatory codes and give support through enforcement." According to the Bertelsmann Foundation text, if definitively private and public regulatory bodies have to work together, the scope of each intervention must be clearly distinguished. Self-regulation must be independently established by the private sector. The role of the public authority is to promote the self-regulatory initiatives from outside and to enforce if necessary the decisions taken by these self-regulatory bodies.

We now return to the conclusion reached in the CDT text. Surprisingly it contrasts with the 'self regulatory model' and 'the user empowerment model'. We believe that is more accurate to consider that 'user empowerment' (see § 5) is only a conceptual element which can be included (or not)[85] in the self-regulatory or coregulatory paradigms (but not in the pure public regulation one).

8.2. Identification of the possible roles of each partner in coregulation

Coregulation is an ambiguous concept since it covers so many different mechanisms and areas (see § 3.1). Thus our intention is now to try to better identify the possible roles of each partner and their possible cooperation in a process of co-regulation of the Internet. We will set out a non exhaustive list of tasks which could be involved in such a process. Among these tasks, some have been already included in an effective joint regulation (e.g. in Australia),[86] others have been suggested or envisaged (e.g. by the Bertelsmann Memorandum [1999] or in USA).[87] and others are put forward for the first time here.

We will take into account the possible players: private sector or public authorities (state or international organization). We will also propose that three levels of action be distinguished. The first level, the most important as regards the user empowerment and rightly praised by CDT, concerns the mechanisms put at the disposal of each individual for exercising his/her freedom. At this level, we will analyse, in particular, the problem of labelling and filtering mechanisms. The second level, emphasized by the Bertelsmann Foundation Memorandum, is the collective answer given by the sector itself in order to provide solutions when the mechanisms of the first level are insufficient or inadequate. The third level concerns the final answer to be given both by the legislature and the judges.

Thus, we will merely outline a grid of analysis of this new paradigm (*see table 8*). In this grid we will try to locate correlated tasks by different players (inside a level) on the same lines. We do not consider this grid as the perfect solution to be implemented. Nevertheless, we will take advantage of this analysis to outline our opinion on some of the possible elements of coregulation.

8.2.1. First level of action: filtering and labelling techniques

Concerning the first level, the development both of various filtering techniques and of labelling systems and activities is the best method of providing (in a totally decentralized manner) a solution that will take into account and respect the infinite diversity of opinions, cultures and sensitivities of the people throughout the world.

8.2.1.1. Role of the private sector

The private sector will play the first role concerning *the development and financing of these products*[88] and services. It is the role of the private sector to develop and finance, within a competitive environment, value-neutral software and products capable of supporting the rating and filtering activities (in particular, we may refer to new developments such as software that takes into account the context of a picture or text, or, software that provides the user with the possibility of adding specific details such as their own personal 'green/ white' lists). The US Commission on Child Online Protection recommends, in particular, (2000 p.42) that "industry take steps to improve child protection mechanisms, and make them more accessible online." It is the role of services providers but also of churches, unions, parents' associations, private or public youth protection associations, schools, etc. to offer rating services[89] in employing the platforms developed by the software and filtering systems producers.

The role of the private sector is also *to achieve a good marketing of its services* on a scale which makes the use of these products and services significant. So, a critical mass of labelled Internet services might be obtained. There is also a

clear need for promotion of labelling and filtering systems on a national or language group basis.

On the other hand, in the Australian example, several other obligations[90] are imposed on the private sector: first, there is the obligation *to provide the users with filtering tools and information*[91] *about these tools* and then, in the framework of the Internet Industry Codes of practice,[92] *to provide a mechanism of product/service approval*[93] and *also to encourage commercial content providers to use appropriate labelling systems.* As for the US Commission on Child Online Protection (2000 p.46), it claims that the adult industry "should pursue efforts to encourage web sites to self-label and should provide incentives[94] for them to do so."

8.2.1.2. Role of the public authorities

The diversity of rating services has to be supported and it is quite obvious that the role of the State is to encourage the development of the filtering and labelling techniques, to promote their use by the citizens through appropriate educational programmes and to ensure a certain pluralism corresponding to the attempts of the different groups of citizens. Furthermore, it is possible to envisage that public regulation requires these private initiatives to be transparent as regards the criteria used for the selection and even the 'black' lists to block,[95] the methods followed and the persons in charge of the system.[96] One could imagine that a public mechanism of approval or certification (e.g. logos, …) would be put at the disposal of the firms which voluntarily want to see certain fixed qualities of their system recognized. It also seems that certain measures must be foreseen against mislabelling[97] since this practice may deeply affect the confidence of the Internet users and cause the Internet users harm. Moreover, price control might be exercised by the State particularly as regards the possibility of incorporating filtering techniques as a basic service of the browser without additional costs.

The State could *also impose upon ISPs to provide users with filtering tools and information about these tools.* This obligation is already included in the new regulatory regime in Australia, as quoted in § 8.2.1.1.

On the other hand, public organizations could *make available relevant information to be included in lists*. This has been suggested by the US Commission on Child Online Protection (2000 p. 9 and 43-44).[98] More concretely, the Bertelsmann Foundation (2000) announced that "Germany's BKA (federal criminal investigation department) will make a list of known Nazi sites available to the ICRA filter system in the form of a negative list."

Finally, the state would *provide schools or other educational agencies with incentives to use filtering techniques*. One should note here that a US Bill[99] regarding the purchase of computers used for Internet access is currently being introduced in order to forbid the provision of any funds to schools or other educational agencies "unless such agency or school has in place, on computers that are accessible to minors, and during use by such minors, technology which filters or blocks: (1)Material that is obscene; (2)Child pornography; (3)Material harmful to minors."With regards to the question of *interoperability* of the different rating systems, it would have *to be analysed and encouraged* by international public organizations since it will allow each Internet user throughout the world a better knowledge of the meaning of the various criteria used by the multiple labelling services.[100]

8.2.1.3. Comment

If, for reasons expressed above, this first level is the most important, it is quite obvious that the solutions provided are not sufficient. For example, it would be contrary to the freedom of expression to a label on each web site. It would be contrary to the Data Protection requirements to forbid the development of anonymous mail and web sites on the Net. Secondly, as previously stated (see § 7.1), due to the permanent evolution of the content of each web service, the labelling services might not offer a perfectly secure system. That is why other levels of action must be considered.

8.2.2. Second level of action: first response to the insufficiencies of level 1

The second level is a response to level one's insufficiencies.

8.2.2.1. Role of the private sector

A collective answer is proposed through *codes of conduct or practice,*[101] *hot line*[102] *mechanisms and various private sanctions* like blocking of infringing web sites, publication of black lists, etc.This answer might be offered individually by an IAP or an ISP or jointly by a consortium of different providers at regional, European or global level.This second level offers complementary solutions to the first level. So, if I discover racist discussions in a forum, I can alert the I.A.P or an association of IAPs. or an ADR through a hot line mechanism and very efficient measures might be taken to stop this illegal action.

On the other hand, it is worth noting a recommendation made by the US Commission of the Online Child Protection (2000) : "government and Industry should effectively promote acceptable use policies."(p. 41).Acceptable use policies mean: "Establishment by a parent or an institution (school or library) of rules regarding the types of materials that may be accessed.Typically, such policies would be enforced by means of denial of further access in the event of a violation." (p. 36). The main fear as regards this second level of control is the over-censorship it might create since the alerted IAP might be urged to act in order to avoid any problem with the "plaintiff" even if eventually it is found that there is no illegal or harmful content. The risk of action on the basis of a *prima facie* infraction is high. That is why, certain limits must be imposed on the self-regulatory solutions.

8.2.2.2. Role of the public sector

First, it must be clear that the possible sanctions must be taken only according to a certain procedure which does respect the basic principle of a fair process.Thus, the US Digital Millennium Copyright Act (DMCA)[103] has enacted the obligation for the IAP or other intermediary services to set up a procedure of "notice and take down notice" plus a "put-back procedure".[104] This procedure deals with complaints about copyright infringements but it would be usefully extended to illegal or harmful content. First,

it requires complaints to be accompanied by specific details and a signature and, secondly, it requires that the alleged violator be notified before any action is taken. Other requirements may be proposed: first, the transparency of the criteria and followed procedure must be ensured. The concrete implementation of the criteria and of the procedure must also be subject to possible control.[105] Except for provisional decisions in cases of obvious infringements,[106] the setting up of Alternative Dispute Resolution Mechanisms[107] respecting the main principles of a fair process[108] is needed before taking definitive sanctions or decisions. Secondly, Data Protection principles and competition must be fully respected as regards the establishing and functioning of the self-regulatory provisions and jurisdictional mechanisms.

On all these points, the Australian case may be quoted. First, the Australian State has required the Internet Industry Association (IAA) to develop codes of practice. The 'IAA Internet Industry codes of Practice' have been registered by the Australian Broadcasting Authority (ABA) on 16 December 1999.[109] They aim mainly to facilitate end-user empowerment.

We think that the role of the State should be, through suitable legislation, to *promote and eventually to approve appropriate self-regulatory solutions*. Doing that, it is quite obvious that the State will have to *remind the self-regulators of the limits of their* actions Moreover,Article 10 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms clearly asserts that any limits as regards the freedom of expression must have legislative grounds, must be specified and limited to what is strictly needed to achieve the specific public interest objectives pursued and described by the legislation.[110] If the private self-regulators might help as regards the pursuing of these objectives, their possible action must respect these limits.[111] On the other hand, as suggested by the Bertelsmann Memorandum (1999), the State should *cooperate with the national hotline*. And as cited above, in cooperation with industry, it should promote acceptable use policies (cf. Commission of the Online Child Protection, 2000).

Moreover, *national hotline cooperation* should be encouraged by International organizations.

8.2.3. Third level of action: final answer to the insufficiencies or the 'latest word'

The third level is the action by the public authorities themselves and the possible cooperation of the private sector to this action. The privilege of the official jurisdictions is that they keep the latest word. It means that no self-regulatory solution might hinder or restrict the right of a person or a body to go before a Court or an administrative body, *either to judge the problem* in case of illegal or harmful content, *or,* according to the *exequatur* procedure, in case of private arbitration*, to check if the self-regulatory solution effectively respects the main principles of Society*, i.e. public order. In this domain, a recent case[112] is quite relevant: on 20 November 2000, "a French court has ruled that US-based Yahoo, Inc. is to be held liable under French law for allowing French citizens to access auction sites for World War II Nazi memorabilia. The court ruling on Monday subjects Yahoo to fines in excess of 100 000 francs (US$12 853) per day unless it installs a keyword-based blocking system that prevents French citizens from seeing the offending Yahoo sites." (Centre for Democracy and Technology (CDT), November 21 2000).

Then, it is the role of the State, after having determined the illegal character of certain content through appropriate jurisdictional means, to *take any appropriate tools in order to prevent any access to these contents* and, in that context, *to impose certain duties to the on line intermediaries*. It is worth noting how these requirements have already been implemented in an example of coregulation: "Internet Content Hosts in Australia must take down content that has been the subject of a complaint to the ABA, and the ABA deems the content to be in breach of Australian law [...] There are heavy penalties for ISPs for non-compliance." (Internet Industry Association, December 20 1999 - updated February 2000) This solution to sue the supposed infringing internet service before the ABA does not exclude the possibility of going before another jurisdiction including a private ADR or another official jurisdiction.[113] The main objective of intervention by an official jurisdiction is ultimately to avoid any private censorship and to impose on all the Internet service providers the obligation of blocking any infringing content of which they are aware. One should note also the decision of UK Yahoo! "to employ a Yahoo! 'inspector' charged with ensuring that yahoo! Messenger system is not polluted with paedophile content." (Barry & McAulliffe, 2000). UK Yahoo! also promised that, at the request of organizations such as Childnet International and the police, it may be willing to abolish chat-rooms because of the threat of paedophiles. Still more recently, US Yahoo said "that it would try more actively to keep hateful and violent material out of its auctions, classified sections and shopping areas." (Guernsey 2001) Indeed it will use a software "that that automatically reviews information that sellers are trying to post on the Yahoo Web site. If the software detects something in the submission that appears to violate the company's standards, the seller will immediately receive a message with links to Yahoo's terms of service. The seller can then revise the listing or appeal to Yahoo's staff for human review." (Guernsey 2001).

Another possible action of the public authority is *to request the cooperation of the private sector in the fight against illegal content.* As we have pointed in § 6.3, many of the recent laws have made this cooperation mandatory and required that public telecommunication services providers (I.A.P, hosting providers, Certification Authorities and intermediary services like search engines) both keep systematic records on the different uses of their services and check the real identity of their subscribers. Much of this legislation does not respect the limitations imposed by the Council of Europe Draft Convention on Cyber-crime (2000) and its case law since they are trying to legitimate disproportionate means of processing personal data with regard to the public interest objectives. Some Acts (e.g. the Belgian one) require that the telecommunication service providers store the data about the different uses of Internet by subscribers for 12 months (e.g. the web sites and the pages visited, the moment, the duration of the visit, the key-words selected as regards the uses of a search engines,) and allow the police authorities access to this data even if there is no specific case against a particular person. We think that *this kind of mandatory cooperation creates large risks to a global network surveillance and exceeds what would be acceptable from a data protection perspective.* National police cooperation should be encouraged by international organizations.

Table 8. Grid of analysis of Coregulation: the different levels of action, some possible roles and corresponding players.

LEVELS OF ACTION	PLAYERS AND	THEIR ROLES	
	PRIVATE SECTOR	PUBLIC AUTHORITIES	
		STATE	INTERNATIONAL ORGANIZATION
Level 3: Final answer to the insufficiencies	•To cooperate with public authorities to fight illegal content	(Court or administrative body:) •Either to judge the problem or to check if the self-regulatory solution effectively respects the main principles of Society; •To request private sector cooperation in the fight against illegal content; •To request the private sector to take any appropriate tools in order to prevent any access to these contents; and •In that context, to impose certain duties on the online intermediaries.	• To encourage national police cooperation
Level 2: First response to the insufficiencies of Level 1	•To develop codes of conduct/practice •To promote acceptable use policies/family contract[114] •To be responsible for various sanctions •To create and finance[115] hotlines	• To promote (through legislation) and, eventually, to approve/register appropriate self-regulatory solutions (particularly: private sector codes of conduct/practice) [116] • To promote acceptable use policies/ family contract • To remind the self-regulators of the limits of their actions • To cooperate with national hotlines	• To encourage national hotlines
Level 1: Filtering and labelling techniques	•To develop and finance the techniques • To provide the users with filtering tools and information about those tools; •(in the framework of codes of conduct/practice) to provide a mechanism of product/service approval; •to obtain good marketing of their services. • (In the framework of codes of conduct/practice)[117] to encourage commercial content providers to use appropriate labelling systems.	• To encourage the development of the labelling and filtering techniques • To require ISP to provide the users with filtering tools and information about those tools • To promote the use of technology by the citizens (notably through an appropriate educational programme) to foresee certain measures against mislabelling. • To ensure a certain pluralism • To require transparency from private initiatives • To provide a mechanism of filtering service approval • To control prices • To make available relevant information to be included in black (/white) lists and used either on a voluntary basis by people or by filtering services[118] • To provide schools or other educational agencies with incentives to use filtering techniques.[119]	• To encourage rating system interoperability

9. CONCLUSIONS

The official texts of the European Union about illegal and harmful content regulation on the Internet show an evolution. They begin (before 98) by supporting private sector leadership, then (98-99) they encourage private — public cooperation and finally (since 2000) they give more investigation power to the state and at the same time limit Internet actor liability. Clearly these European texts differ from the corresponding US ones in the importance they always give to the respect for cultural diversity.

The concept of 'parent empowerment' linked to Internet content governance appeared in US from 1995 as a reaction by the Internet industry to the threat of the public censorship. It is indeed the leitmotif of the libertarian associations and of advocates of 'free speech' which are so powerful in US It implies that parents – not the State- are considered in charge of child protection on the Internet. This concept has been quickly and definitively adopted, first by the US government and then by the European Union. It is also put forward both by the Bertelsmann[120] Foundation Memorandum entitled 'Self-regulation of Internet Content' (September 1999) and by the text of the US Centre for Democracy and Technology (CDT)[121] (October 1999) answering to this Memorandum.

The corollary of the concept of 'user empowerment' is the use of Internet filtering techniques by parents. Concerning these techniques, we suggest a framework to help understanding and we stress the importance of the labelling techniques (notably with PICS) as an effective means of empowering parents. We refer again to the conclusions of our survey on 44 off-the-shelf filtering services from the filtering criteria viewpoint.[122] This survey showed that the market alone is unable to answer the need for a variety of European user opinions and cultures. And contrary to the view of some free speech US lobbies, *we would like to stress that 'user empowerment' also basically implies that all users can make value judgements particularly without having to refer to the judgements of American firms and industry*.

'User empowerment' is a conceptual element which can be included (or not)[123] in the self-regulatory or co-regulatory paradigms (but not in the purely public regulation one). It includes the right of the Internet user to be informed and educated as regards the risks linked to both the Internet and the available Internet filtering and labelling tools. It also involves the user's right to dispose of efficient, diverse, transparent, affordable and adapted technologies and services to answer his need for protection. On the other hand, it involves the user's right to have efficient mechanisms to report any infringement and, in these cases, to have rapid, proportionate and adequate sanctions. To ensure these rights, public authorities must intervene. But the private sector alone is in charge of providing competitive, flexible and evolutionary solutions which cope with the cultural, philosophical and ideological diversity. The role of the public authority is both ancillary and essential *vis-à-vis* the private sector. Ancillary, because the public authority's intervention might never be a substitute for private intervention[124] but must promote this intervention as a way of ensuring the Internet user's rights. Essential, because the main role of the State is to constantly bear in mind the limits imposed by the fundamental human rights: privacy and freedom of expression, to assert the Internet user's rights to be protected against illegal and harmful content by creating an appropriate regulatory framework (including by promoting self-regulatory measures). In that sense, *we plead strongly in favour of a coregulatory approach.* This model (even if not called as such) is advocated by the Memorandum and feared by CDT. It can be considered as including three levels of action: the first one concerns filtering and labelling techniques, the second one is a first response to the insufficiencies of level one and the third is the final answer. At each level, there are various possible roles which have to be attributed to the private sector or the public authorities in order to make them collaborate. There are several possible choices to implement the paradigm. *We think that this joint regulation of Internet content is necessary and promising but must be kept within some limits to avoid the risk of a global surveillance of the networks*.

As the US Commission on Child Online Protection concluded in its report to the Congress (October 2000 p. 9)[125]: "After consideration of the information gathered through hearings and comments filed by a wide range of parties, the Commission concludes that no single technology or method will effectively protect children from harmful material online. Rather, the Commission determined that a *combination* of public education, consumer empowerment technologies and methods, increasing enforcement of existing laws, and industry action are needed to address this concern."

Marie D'udekem-Gevers Institut d'Informatique, University of Namur, Belgium
Yves Poullet, Centre de Recherche Informatique et Droit (CRID), University of Namur, Belgium.

This paper has been produced thanks to a financial support of the Belgian 'Federal Office for Scientific, Technical and Cultural Affairs' (OSTC), within the framework of the programme 'Pôles d'Attraction Interuniversitaires (PAI IV)'. The authors thank N. Condon for having corrected their English text.

FOOTNOTES

[56] See European Union, Internet Action Plan (IAP), IST 2000 conference in Nice, France (6 — 8 November).

[57] See, for example, GetNetWise or The Internet Filter Software Chart.

[58] See, for example, Cranor, Resnick, & Gallo, 1998, or Ryan & Triverio, 1999.

[59] See also Marie d'UDEKEM-GEVERS, 1999.

[60] W3C was founded in 1994 to develop common protocols to enhance the interoperability and lead the evolution of the WWW. It is an international industry consortium, jointly hosted by the MIT's (Massachusetts Institute of Technology) (US), INRIA (Institut National de Recherche en Informatique et en Automatique) (Europe) and the Keio University Shonan Fujisawa Campus (Japan). Initially, the W3C was established in collaboration with CERN, where the Web originated, with support from DARPA and the European Commission.

[61] Surprisingly, the Mathonet et al. study (1999) which is entitled 'Review of European Third- party filtering and rating software and services' is however not limited to third party (filtering and) ratings as defined here but also includes what we call here 'filtering on the basis of black lists of URLs'.

[62] Strangely, the CDT text defines the word labelling as 'self-rating' and links it with the so- called 'cooperative filters' because it requires the cooperation of content providers.

[63] See P. Overell 1996.

[64] See W3C, PICS Frequently Asked Questions.

[650 See Konrad, 2000.

[66] See d'Udekem-Gevers, 1999.

[67] Chat and email are not considered here but they are well known to be potentially dangerous for children (see for example Launet, 2000): "Recent research from the United States appears to suggest that nearly one in five young Internet users has been the victim of a sexual approach or solicitation online." (Internet Crime Forum IRC sub-group, October 2000)

[68] The criteria used for rating are the same used later for filtering.

[69] The needed relevance of a filtering system to the different cultural background of member states is also stressed by Kerr (2000 p.3 & 37-38).

[70] See Kerr, 2000, p. 4 & 5: "Self-labelling and filtering systems have the technical and theoretical potential to meet the needs of European consumers […] The establishment of a viable system(s) is dependent on more content being labelled and/or on a workable combination of self-labelling and third party rating."

[71] A profile is called a 'template' in the Memorandum. See Kerr 2000 for more on the profiles for future use.

[72] Our italics.

[73] See the discussion of Weinberg J. 1997 on this subject.

[74] Or by content providers as suggested by the US Commission on Child Online Protection (2000). See § 8.2.1.

[75] Grainger's analysis (1999 p. 53- 54) states "Whereas in the United States of US Constitution First Amendment allows the free speech lobby to dominate discussion about self-regulation, other countries with healthy democratic systems and vibrant process of open expression are able to seek a more appropriate balance between the right to free expression *and the right of communities to nurture national and local cultures and to protect children from harmful content…*"

[76] See also § 8.2.

[77] CPSR stands for Computer Professionals for Social Responsibility. It is a US 'public-interest alliance of computer scientists and others concerned about the impact of computer technology on society'.

[78] See Kerr 2000, p.6.

[79] According the kerr's analysis (2000, p. 3) the problem of unrated sites is the 'main problem' of the current state of filtering and rating techniques.

[80] Nevertheless, self rating has also been recommended by the Action Plan approved by the 'First World Summit for Regulators' (30 November - 1 December, Paris, UNESCO).

[81] See Kerr 2000, p.39-40.

[82] This is the system available in U.S under the False and Deceptive Statement Act, which grants the right to provide an injunction in case of false or deceptive statement to the Federal trade commission (F.T.C.).

[83] This is also one of Kerr's conclusion (2000 p.43).

[84] Compare with our assertion: "We should like to stress the State's vital obligation to intervene at a time when in our opinion deserting the Internet and withdrawing from the field of regulation to such a point that it no longer even decides the general framework, would notably put at a risk public order, fundamental liberties and other basic values." (Poullet 2000).

[85] In this case, the private sector would be responsible for the protection of minors.

[86] Since the Australian Broadcasting Services Act 1992 as amended is based on this approach, we will make extensive reference to the Australian solution. It is worth noting that the Australian texts use the term 'coregulation' to refer to their new regulatory regime.

[87] Cf. Departments of Labour, Health and Human Services, and Education, and related Agencies, H.R.4577— Appropriations Act, 2001

[88] These two tasks are envisaged e.g. by the Bertelsmann Memorandum, 1999 (p. 56).

[89] The system should have to support the development of profiles established by these associations considered as trusted third parties. The individuals must have the possibility of downloading these profiles (see § 7.2.3 and 7.2.4 and table 7) according to their cultural, philosophical or ideological preferences.

[90] See Internet Industry Association, December 20 1999 - updated 2000 and Internet Industry Association, December 16 1999 — updated 22 December. It is worth noting that according to the Australian regulatory regime: "ISPs will not be required to evaluate the content themselves" and "are not required "to ensure that end-users install or operate the filters".

[91] In this domain, the US Commission on Child Online Protection (2000, p. 41) recommends that "the private sector – industry, foundations and public interest organizations – provide support for an independent, non-governmental testing facility for child-protection technologies."

[92] See Internet Industry Association, 1999.

[93] A list of filters approved by the Internet Industry Association is included in the Internet Industry Codes of Practice. [This list is not endorsed by ABA (see Lebihan 2000).]

[94] One should remember (see § 7.3.1 and *Table* 7) that according to the suggestions of the Bertelsmann Foundation, State should be responsible for the creation of incentives for rating.

[95] The US "Copyright Office said it should be legal for users to access such lists, in part so people can criticize and debate them." (Wilde Mathews, October 27 2000)

[96] The Commission on Child Online Protection (COPA) Report to [US] Congress (Oct. 2000) estimates that: "Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies".

[97] Cases of mislabelling (and thus 'overblock') have already been condemned. See, for example, the famous 'breaking of Cyber Patrol' by Jansson & Skala (2000). See also Bowman (2000), Lebihan (2000) and Finkelstein (2000). The Cyber patrol case is of interest. The publication of the list of blocked Web sites by people who had bypassed the weak security measures developed by Cyber Patrol had revealed that the Cyber patrol filter was blocking certain Web sites for competition reasons and not for their illegal or harmful content.

[98] Cyber patrol has sued the infringers for violations of the Digital Millenium Copyright Act of 1998 (see Act, infra § 8.2.2.2) which grants protection for the persons who have installed technical protection measures in order to prevent copyrighted works. According to the arguments of Cyber patrol, the list of blocked Web sites was copyrightable. In our opinion, this argument is not acceptable since the criteria used by the filtering operators must be transparent and that certain control may be exercised about their effective respect. It would be too easy to take the argument of copyright in order to prevent any access to the list of blocked Web sites.

"The Commission recommends that state and federal law enforcement make available a list, without images, of Usenet newsgroups, IP addresses, World Wide web sites and other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material. This information may be

used to identify obscene materials or child pornography under the control of ISP or content provider."

[99] See Section 304 of the Departments of Labor, Health and Human Services, and education, and related Agencies, H.R.4577- Appropriations Act, 2001. See also excerpts of this Act made available by CDT at <http://www.cdt.org/legislation/106th/speech/001218cipa.pdf >.This act was passed by both the House and Senate on December 15 2000 (see Center for Democracy and Technology, 18 December 2000).

[100] Kerr (2000 p. 44) draws a similar conclusion when he pleads for "an international standards body to co-ordinate the process of developing the systems and to monitor their interoperability, quality and security."

[101] The Commission on Child Online Protection (2000 p. 44):"urges the ISP industry to voluntarily undertake 'best practices' to protect minors."

[102] "Facilities for easy reporting of problems to the parties who can address them, either online or via telephone. Such hotlines would bring problems to the attention of both relevant government authorities and private sector groups that can act in response to reported problems." (Commission on Child Online Protection, 2000 p. 32)

[103] See Senate and House of Representatives of the United States of America, 1998. According to the Sect. 512 (c) 1 a hosting service provider who expeditiously blocks access to material if he receives a notification of a rights holder claiming that the content concerned infringes his copyrights, he will avoid liability.

[104] According to the Sect.512 (c) and (g) of the US Digital Millenium Copyright Act, the person whose material has been removed has the right to object and to have his material put back on the Net. See Julia-Barcelo, 2000.

[105] See the Cyber Patrol case (supra) where the filtering operator denies the right of a third party to access the list of blocked Web sites in order to verify its compliance with filtering criteria.

[106] In these cases, a notice must be sent immediately to the public authorities (see level 3).

[107] See § 3.1.1.

[108] These principles, enacted by article 17 of the European Parliament and Council Directive on E-commerce (2000), are the following : impartiality and qualification of the "judges", accessibility and convenience for Internet users, transparency of the functioning and of outputs, adversarial procedure, possibility of representation6

[109] See also, the annex of the (E.U.) Council Recommendation of 24 September 1998 (which fixes the minimal requirements of the codes of conduct concerning Internet content and the protection of minors) and the following COPA recommendations (2000) : "Government and industry should effectively promote acceptable use policies".

[110] This Article asserts: (1)"Everyone has the right to freedom of expression.This right shall include freedom to hold opinions and to receive and impart information and ideas without the interference by public authority and regardless of frontiers.This Article shall not prevent States from requiring licensing of broadcasting, television or cinema enterprises "

(2)"The exercise of these freedoms, since it carries with it duties and responsibilities, may not be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic Society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for the prevention of disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Regarding Article 10 of the Council of Europe Convention and the similar provision included within the Universal Declaration of Human Rights (art.19), see Global Internet liberty Campaign (GILC), Sept.98. A summary of the case law of the European Court of Strasbourg may be found in Lester 1993.

[111] In our opinion, Article 10 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms is also applicable *vis-à-vis* private authorities when these private authorities censor illegitimately the content on the basis of an explicit or implicit delegation of powers by the public authorities.

[112] See 'Tribunal de Grande Instance de Paris, Ordonnance de référé du 20 Novembre 2000'.

[113] It is not obvious that an administrative authority, competent as regards audio-visual services, is the most appropriate to solve questions linked with the protection of minors. Undoubtedly, the competence of traditional criminal courts acting urgently would be a better solution.

[114] cf. Commission on Child Online Protection, 2000.

[115] cf. the Bertelsmann Memorandum (1999 p. 56).

[116] cf. the Australian example.

[117] See also § 13 of the Hong Kong Internet Service Providers Association's Code of Practice - Practice Statement on Regulation of Obscene and Indecent Material.

[118] cf. the "Germany's BKA (federal criminal investigation department) example as mentioned in Bertelsmann 2000.

[119] cf. Departments of Labour, Health and Human Services, and Education, and related Agencies, H.R.4577- Appropriations Act, 2001.

[120] Bertelsmann is a media giant.

[121] CDT is a non-profit organization dedicated to promoting democracy in general and, in particular, free expression.

[122] Three main questions have been asked: Who has been responsible for defining the filtering criteria? Who has used them to classify or rate web sites? How can they be customized?

[123] In this case, the private sector should be in charge of the protection of minors.

[124] See the 1998 UN Report of the Special Rapporteur, Mr. Abid Hussain (last § of C. The impact of new information technologies): "The Special Rapporteur is of the opinion that the new technologies and, in particular, the Internet are inherently democratic, provide the public and the individual access to information sources and enable all to participate actively in the communication process. The Special Rapporteur also believes that action by States to impose excessive regulations on the use of these technologies and, again, particularly the Internet, on the grounds that control, regulation and denial of access (necessary to preserve the moral fabric and cultural identity of societies) is paternalistic. These regulations presume to protect people from themselves and, as such, they are inherently incompatible with the principles of the worth and dignity of each individual. These arguments deny the fundamental wisdom of individuals and societies and ignore the capacity and resilience of citizens, whether on a national, State, municipal community or even neighbourhood level, often to take self-correcting measures to reestablish equilibrium without excessive interference or regulation by the State."

[125] Although the Commission on Child Online Protection recommendations do not use the word coregulation, they are clearly in favour of this regulation paradigm.